计算机应用数学 复习提纲

一、概率论基本知识

事件及其相应概念 略

常见的概率模型

不放回抽样：超几何分布： $X \sim H(n, M, N)$

为离散分布模型，概率取值为$P(X=m)=\frac{\binom{M}{m}\binom{N-M}{M-m}}{\binom{N}{n}}$

有$EX=\frac{nM}{N}, Var(X)=\frac{nM}{N}(1-\frac{M}{N})\frac{N-n}{N-1}$

直观理解：不放回抽样，N个产品中不合格产品有M个,从中任取n个，有m个不合格品的概率

更直观理解：N个物品分两类，A类有M个，从中取n个，其中A类取到m个

放回抽样：二项分布： $X \sim B(n, p=M/N)$

概率取值$P(X=m)=\binom{n}{m}(\frac{M}{N})^m(\frac{N-M}{N})^{n-m}$

$EX=np, Var(X)=np(1-p)$

直观理解：N个产品，M个不合格品，从中有放回任取n个，有m个不合格品概率

盒子模型： n个**不同**的球放入N个**不同**的盒子里，每个盒子所放球数不限，则

恰有n个盒子中各放一球的概率$P(X=n)=\frac{P(N,n)}{N^n}=\frac{N!}{N^n(N-n)!}$

应用：生日问题

配对模型： n个人n顶帽子，任意拿取，至少一人拿对帽子的概率

$$P=1-\frac{D_n}{n!}=1-\frac{1}{2!}+\frac{1}{3!}-\cdots+(-1)^{n-1}\frac{1}{n!}\to 1-e^{-1}$$

条件概率

$P(B|A)=P(AB)/P(A)$

三大公式：乘法公式，全概率公式，贝叶斯公式

乘法公式：若$P(A_1A_2\cdots A_{n-1})>0$，则

$$P(A_1A_2\cdots A_n)=P(A_1)P(A_2|A_1)\cdots P(A_n|A_1A_2\cdots A_{n-1})$$

题例：100个零件中有10个不合格，从中不放回取，求第三次**才**取出不合格品的概率

解：分解为：第一，第二次合格，第三次不合格，用乘法公式

$$P(YYN)=P(Y)P(Y|Y)P(N|YY)=\frac{90}{100}\times\frac{89}{99}\times\frac{10}{98}$$

全概率公式：样本空间一组分割$\Omega=B_1\cup B_2\cup\cdots\cup B_n, B_iB_j=\Phi, P(B_i)>0$

则$P(A)=\sum_{i=1}^{n}P(AB_i)=\sum_{i=1}^{n}P(B_i)P(A|B_i)$

例：摸彩模型：n张彩票中有k张中奖，不放回地摸取，则第i次摸到奖券的概率

$$P(A_i)=k/n$$

解：易见$P(A_1)=k/n$

$$P(A_2)=P(A_1)P(A_2|A_1)+P(\bar{A}_1)P(A_2|\bar{A}_1)=\frac{k}{n}\cdot\frac{k-1}{n-1}+\frac{n-k}{n}\cdot\frac{k}{n-1}=\frac{k}{n}$$

以此类推即可。

贝叶斯公式：样本空间一组分割$\Omega=B_1\cup B_2\cup\cdots\cup B_n, B_iB_j=\Phi, P(B_i)>0$

则$P(B_i|A)=\frac{P(AB_i)}{P(A)}=\frac{P(B_i)P(A|B_i)}{P(A)}=\frac{P(B_i)P(A|B_i)}{\sum_{j=1}^{n}P(B_j)P(A|B_j)}$

其中$P(B_j)$称为先验概率，$P(B_j|A)$称为后验概率

核心思想：用结果推原因

例：机器状态良好时，产品合格率为98%; 发生故障时，合格率为55%;

每天早上启动机器时，机器状态良好的概率为95%

则在已知早上第一件为合格品时，机器状态良好的概率是多少?

解：$A=$"第一件产品合格"，$B=$"机器状态良好"

则$P(A|B)=0.98, P(A|\bar{B})=0.55, P(B)=0.95, P(\bar{B})=0.05$

由Bayesian eq. $P(B|A)=\frac{P(A|B)P(B)}{P(A|B)P(B)+P(A|\bar{B})P(\bar{B})}=0.97$

新冠阳性与确诊题例：作业2

独立性

定义: $P(AB)=P(A)P(B)$

若$P(A)>0$，则等价于$P(B|A)=P(B)$

两两独立：$P(A_iA_j)=P(A_i)P(A_j)$

相互独立：事件$A_1,\cdots,A_n$满足两两,...,nn独立，则称它们相互独立。

例：两射手轮流对同一目标射击，甲先射，谁先击中谁获胜，甲，乙每次命中概率分别为α,β,求甲获胜概率

$$P(\text{甲胜})=\alpha+(1-\alpha)(1-\beta)P(\text{甲胜})\Rightarrow P(\text{甲胜})=\frac{\alpha}{1-(1-\alpha)(1-\beta)}$$

元件工作：串联：$P(A_1A_2)=p_1p_2$ 并联：
$P(A_1\cup A_2)=1-(1-p_1)(1-p_2)=p_1+p_2-p_1p_2$

桥式系统：见作业1

离散随机变量

定义：定义在样本空间Ω上的实数单值函数$X=X(\omega)$

取值为可数称为离散随机变量，取值充满某个区间称为连续随机变量

常用分布： 二项分布&超几何分布上面已经给出

直观：n次Bernolli试验中成功的次数

直观：不放回抽样模型

泊松分布：$X\sim P(\lambda), P(X=k)=\frac{\lambda^k}{k!}e^{-\lambda}$，$EX=Var(X)=\lambda$

直观：一事件以密度λ随机且独立出现，则在单位时间内随机事件发生k次的概率

二项分布的泊松近似：n重Bernoulli分布，若$np_n \to \lambda$

则$\binom{n}{k}p_n^k(1-p_n)^{n-k} \to \frac{\lambda^k}{k!}e^{-\lambda}$

几何分布：$X \sim Ge(p), P(X=k) = (1-p)^{k-1}p, EX = \frac{1}{p}, Var(X) = \frac{1-p}{p^2}$

直观：n次伯努利试验中，试验k次得到第一次成功的概率

无记忆性：$P(X>m+n|X>m) = P(X>n)$

负二项分布：$X \sim Nb(r,p), P(X=k) = \binom{k-1}{r-1}(1-p)^{k-r}p^r, k = r, r+1, \cdots$

直观：伯努利实验，直到r次成功时的所需的试验次数。

拆解为第k次成功，前$k-1$次有$r-1$次成功

$EX = \frac{r}{p}, Var(X) = \frac{r(1-p)}{p^2}$

分布函数和连续随机变量

随机变量X,称$F(x) = P(X \le x)$为X的分布函数,也称累积分布函数 (CDF)

基本性质为1. 单调非减 2.$0 \le F(x) \le 1, F(-\infty) = 0, F(+\infty) = 1$ 3.**右连续**

连续随机变量：随机变量的分布函数$F_X(x)$,若存在**非负可积**函数$f(x)$满足：

$$F(x) = \int_{-\infty}^{x} f(t)dt$$

则称X为连续随机变量，$f(x)$为概率密度函数（pdf）

基本性质为：1.非负性 2.$\int_{-\infty}^{+\infty} f(x)dx = 1$

例：设$X \sim f(x)$, 且$f(-x) = f(x), F(x)$为X的分布函数，则对任意实数$a > 0$,有(B)

A. $F(-a) = 1 - \int_0^a f(x)dx$　　　B. $F(-a) = \frac{1}{2} - \int_0^a f(x)dx$

C. $F(-a) = F(a)$　　　D. $F(-a) = 2F(a) - 1$

解：$1 = F(-a) + \int_{-a}^{a} f(x)dx + \int_{a}^{+\infty} f(x)dx = 2F(-a) + 2\int_0^a f(x)dx$

常用分布： 均匀分布：$X \sim U(a,b), EX = \frac{a+b}{2}, Var(X) = \frac{(b-a)^2}{12}$

$$f(x) = \begin{cases} \frac{1}{b-a}, a < x < b \\ 0, otherwise \end{cases}$$

指数分布：$X \sim Exp(\lambda), \theta > 0, EX = \frac{1}{\lambda}, Var(X) = \frac{1}{\lambda^2}$

$$f(x) = \begin{cases} \lambda e^{-\lambda x}, x > 0 \\ 0, x \le 0 \end{cases}, F(x) = \begin{cases} 1 - e^{-\lambda x}, x > 0 \\ 0, x \le 0 \end{cases}$$

无记忆性：$P(X > s+t | X > s) = P(X > t)$

正态分布：$X \sim N(\mu, \sigma^2), EX = \mu, Var(X) = \sigma^2$

$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}}\exp\{-\frac{(x-\mu)^2}{2\sigma^2}\}$$

标准正态分布$N(0,1)$,此时记$F(x) = \Phi(x), f(x) = \varphi(x)$

Cor: 若$X \sim N(\mu, \sigma^2)$,则$F(x) = \Phi(\frac{x-\mu}{\sigma})$

3σ原则：$P(|X-\mu| < \sigma) = 0.6826, P(|X-\mu| < 2\sigma) = 0.9544,$

$$P(X-\mu|<3\sigma)=0.9974$$

Gamma分布：$X \sim Ga(\alpha,\lambda),\alpha>0,\lambda>0$，$EX=\frac{\alpha}{\lambda},Var(X)=\frac{\alpha}{\lambda^2}$

$$f(x)=\frac{\lambda^\alpha}{\Gamma(\alpha)}x^{\alpha-1}e^{-\lambda x},x\ge 0$$

其中$\Gamma(\alpha)=\int_0^{+\infty}x^{\alpha-1}e^{-x}dx$为$\Gamma$函数

直观：α个相互独立的指数分布的随机变量和

Beta分布：$X\sim Be(a,b),a>0,b>0,EX=\frac{\alpha}{\alpha+\beta},Var(X)=\frac{\alpha\beta}{(\alpha+\beta)^2(\alpha+\beta+1)}$

$$f(x)=\frac{1}{\mathrm{B}(a,b)}x^{a-1}(1-x)^{b-1}$$

其中$\mathrm{B}(a,b)=\int_0^1 x^{a-1}(1-x)^{b-1}dx$为$\mathrm{B}$函数

注意有$\mathrm{B}(a,b)=\frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}$

随机变量函数的分布

离散变量：当X为离散变量时，$Y=g(X)$也为离散变量。

若X分布律为$P(X=x_k)=p_k$,则Y的分布律为$P(Y=y_i)=\sum_{g(x_k)=y_i}p_k$

连续变量：已知连续变量X的密度函数$f_X(x)$,$Y=g(X)$,求$f_Y(y)$

方法：分布函数法，先求分布函数$F_Y(y)$,再求$f_Y(y)$

例：已知$f_X(x)$,求$Y=X^2$的pdf $f_Y(y)$.

$$F_Y(y)=P(Y\le y)=P(X^2\le y)=P(-\sqrt{y}\le X\le\sqrt{y})=F_X(\sqrt{y})-F_X(-\sqrt{y})$$

$$f_Y(y)=F_Y'(y)=\begin{cases}\frac{1}{2\sqrt{y}}[f_X(\sqrt{y})+f_X(-\sqrt{y})],y>0\\0,y\le 0\end{cases}$$

Theorem: $X\sim f_X(x),y=g(x)$为x的严格单调函数，则有反函数$x=h(y)$连续可导，则

$$f_Y(y)=\begin{cases}f_X[h(y)]|h'(y)|,\alpha<y<\beta\\0,otherwise\end{cases},\text{其中}\alpha=\min\{g(-\infty),g(+\infty)\},\beta=\max\{g(-\infty),g(+\infty)\}$$

例：对数正态分布：设$X\sim N(\mu,\sigma^2)$,则$Y=e^X$服从

$$f_Y(y)=\frac{1}{\sqrt{2\pi}y\sigma}\exp\{-\frac{(\ln y-\mu)^2}{2\sigma^2}\},y>0$$

多维随机变量及其分布

二维随机变量

X,Y定义在同一样本空间Ω上，(X,Y)即为二维随机变量，多维随机变量也称随机向量。

联合分布函数：$F(x,y)=P(X\le x,Y\le y)$为(X,Y)的联合分布函数

仍然满足分布函数三条性质。

二维离散随机变量的联合分布律（略）

联合密度函数：若存在非负可积函数$f(x,y)$,s.t.

$$F(x,y)=\int_{-\infty}^{x}\int_{-\infty}^{y}f(u,v)dvdu$$

则称(X,Y)为二维连续随机变量，$f(x,y)$为联合概率密度。

仍然满足密度函数两条性质。

常用分布： 多项分布：每次试验有r种结果$A_1,\cdots,A_r$

记$P(A_i)=p_i,X_i$为n次独立重复实验种出现A_i的次数，则有

$$P(X_1=n_1,X_2=n_2,\cdots,X_r=n_r)=\frac{n!}{n_1!n_2!\cdots n_r!}p_1^{n_1}p_2^{n_2}\cdots p_r^{n_r}$$

直观：多项式定理$(p_1+p_2+\cdots+p_r)^n$的系数

多维超几何分布：N只球分为r类，第i种球有N_i只，任取n只不放回，X_i为取出球中第i种个数

$$P(X_1=n_1,X_2=n_2,\cdots,X_r=n_r)=\frac{\binom{N_1}{n_1}\binom{N_2}{n_2}\cdots\binom{N_r}{n_r}}{\binom{N}{n}}$$

二维均匀分布：$(X,Y)\sim U(D)$

$$f(x,y)=\begin{cases}\frac{1}{S_D},(x,y)\in D\\0,otherwise\end{cases}$$

二维正态分布： $(X,Y)\sim N(\mu_1,\mu_2,\sigma_1,\sigma_2,\rho),\sigma_1,\sigma_2>0,|\rho|<1$

$$f(x,y)=\frac{1}{2\pi\sigma_1\sigma_2\sqrt{1-\rho^2}}\exp\{-\frac{1}{2(1-\rho^2)}[\frac{(x-\mu_1)^2}{\sigma_1^2}+\frac{(y-\mu_2)^2}{\sigma_2^2}-2\rho\frac{(x-\mu_1)(y-\mu_2)}{\sigma_1\sigma_2}\}$$

边缘分布： $X\sim F_X(x)=F(x,+\infty),Y\sim F_Y(y)=F(+\infty,y)$称为边缘分布函数

边缘分布律：$p_i=P(X=x_i)=\sum_{j=1}^{\infty}p_{ij},p_j=P(Y=y_j)=\sum_{i=1}^{\infty}p_{ij}$

边缘密度函数：$f_X(x)=\int_{-\infty}^{+\infty}f(x,y)dy,f_Y(y)=\int_{-\infty}^{+\infty}f(x,y)dx$

由边缘分布一般无法求出联合分布

二维正态分布的边缘分布为一维正态分布

二维均匀分布的边缘分布**不一定**是一维均匀分布

例：(X,Y)服从区域$D=\{(x,y),x^2+y^2<1\}$上的均匀分布，求X的边缘密度$f_X(x)$

解：$f(x,y)=\frac{1}{\pi},x^2+y^2\le 1$,故当$|x|\le 1$时有，

$$f(x)=\int_{-\sqrt{1-x^2}}^{\sqrt{1-x^2}}\frac{1}{\pi}dy=\frac{2}{\pi\sqrt{1-x^2}}$$

条件分布： 条件分布律：$p_{i|j}=P(X=x_i|Y=y_j)=\frac{p_{ij}}{p_{\cdot j}}$

条件概率密度：$f_{X|Y}(x|y)=\frac{f(x,y)}{f_Y(y)}$

条件分布函数：$F(x|y)=\begin{cases}\sum_{x_i\le x}P(X=x_i|Y=y)\\\int_{-\infty}^{x}f_{X|Y}(x|y)dx=\int_{-\infty}^{x}\frac{f(x,y)}{f_Y(y)}\end{cases}$

例：$f(x,y)=\begin{cases}\frac{e^{-x/y}e^{-y}}{y},0<x<\infty,0<y<\infty\\0,\ otherwise\end{cases}$,求$P(X>1|Y=y)$

解：$P(X>1|Y=y)=\int_1^\infty f_{X|Y}(x|y)dx=\int_1^\infty \frac{f(x,y)}{f_Y(y)}dx$

其中$f_Y(y)=\int_{-\infty}^\infty f(x,y)dx=e^{-y}$

则$P(X>1|Y=y)=\int_1^\infty \frac{e^{-x/y}}{y}dx=e^{-1/y}$

随机变量的独立性： 满足以下三条任一，则X与Y独立：

1）$F(x,y)=F_X(x)F_Y(y)$ 2) $p_{ij}=p_{i\cdot}p_{\cdot j}$ 3)$f(x,y)=f_X(x)f_Y(y)$

若联合概率密度有$f(x,y)=g(x)h(y)$，则X与Y独立

对二元正态分布，X与Y独立当且仅当$\rho=0$

n维随机变量： $F(x_1,\cdots,x_n)=\int_{-\infty}^{x_n}\cdots\int_{-\infty}^{x_1}f(x_1,\cdots,x_n)dx_1\cdots dx_n$

其边缘分布有$F_{X_i}(x_i)=F(\infty,\cdots,x_i,\cdots,\infty)$

$f_{X_i}(x_i)=\int_{-\infty}^\infty\cdots\int_{-\infty}^\infty f(x_1,\cdots,x_n)dx_1\cdots dx_{i-1}dx_{i+1}\cdots dx_n$

独立性：X_i之间相互独立，若$F(x_1,\cdots,x_n)=F_{X_1}(x_1)\cdots F_{X_n}(x_n)$

卷积公式： X与Y相互独立，则$Z=X+Y$的密度函数为

$$f_Z(z)=\int_{-\infty}^\infty f_X(x)f_Y(z-x)dx=\int_{-\infty}^\infty f_X(z-y)f_Y(y)dy$$

pf: $F_Z(z)=P(Z\le z)=P(X+Y\le z)$,不妨设可行域$D=\{(x,y):x+y\le z\}$

则$F_Z(z)=\int\int_D f(x,y)dxdy=\int_{-\infty}^\infty[\int_{-\infty}^{z-y}f(x,y)dx]dy$

则$f_Z(z)=F_Z'(z)=\int_{-\infty}^\infty f(z-y,y)dy$

特别的，若X与Y独立，则有$f_Z(z)=\int_{-\infty}^\infty f_X(z-y)f_Y(y)dy$

离散ver. $P(Z=z_l)=\sum_{j=1}^\infty P(X=z_l-y_j)P(Y=y_j)$

建议看一下例题3.5.3，

第3节 多维随机变量及其分布 **第66页**

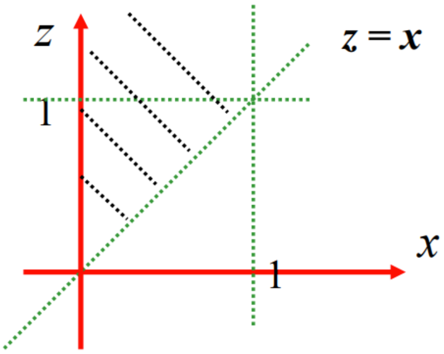
例3.5.3 设 X 与 Y 独立，$X\sim U(0,1)$，$Y\sim Exp(1)$. 试求 $Z=X+Y$ 的密度函数.

解： $X\sim f_X(x)=\begin{cases}1, & 0\le x\le 1\\ 0, & 其\ 它\end{cases}$ $\quad Y\sim f_Y(y)=\begin{cases}e^{-y}, & y>0\\ 0, & y\le 0\end{cases}$

用卷积公式：$f_Z(z)=\int_{-\infty}^{+\infty}f_X(x)f_Y(z-x)\mathrm{d}x$

被积函数的非零区域为：

$0<x<1$ 且 $z-x>0$ (见下图)



因此有

(1) $z<0$ 时 $f_Z(z)=0$;

(2) $0<z<1$ 时 $f_Z(z)=\int_0^z e^{-(z-x)}dx=1-e^{-z}$

(3) $1<z$ 时 $f_Z(z)=\int_0^1 e^{-(z-x)}dx=e^{-z}(e-1)$

分布的可加性：对**独立**的随机变量，

二项分布 $b(n_1,p)+b(n_2,p)=b(n_1+n_2,p)$

泊松分布$P(\lambda_1)+P(\lambda_2)=P（\lambda_1+\lambda_2)$,这里要注意$X-Y$并不服从泊松分布

正态分布$N(\mu_1,\sigma_1^2)\pm N(\mu_2,\sigma_2^2)=N(\mu_1\pm\mu_2,\sigma_1^2+\sigma_2^2)$

伽马分布$Ga(\alpha_1,\lambda)+Ga(\alpha_2,\lambda)=Ga(\alpha_1+\alpha_2,\lambda)$

相互独立的指数分布随机变量之和为伽马分布

变量代换法：若(X,Y)分布已知，(U,V)满足$\begin{cases}U=g_1(X,Y)\\V=g_2(X,Y)\end{cases}$,则$(U,V)$的分布为

$$f_{UV}(u,v)=f_{XY}(x(u,v),y(u,v))|\frac{\partial(x,y)}{\partial(u,v)}|$$

在求解单个随机变量$U=g(X,Y)$的分布时，也可先构造出$V=h(X,Y)$再求边缘分布

作业3：3维随机向量(X,Y,Z)的联合密度函数如下

$$f(x,y,z)=\begin{cases}\frac{1-\sin x\sin y\sin z}{8\pi^3},0\le x,y,z\le 2\pi\\0,otherwise\end{cases}$$

证明X,Y,Z是两两独立而非相互独立的。直接用定义证明即可，$f_{X,Y}(x,y)=f_X(x)f_Y(y)$

随机变量的特征-期望，方差，协方差

数学期望：离散：$EX=\sum_k x_kp_k$ 连续：$EX=\int_{-\infty}^{\infty}xf(x)dx$

若$Y=g(X)$，且$E(g(X))$存在，则$E(g(X))=\begin{cases}\sum_{i=1}^{\infty}g(x_i)P(X=x_i),离散\\\int_{-\infty}^{\infty}g(x)f(x)dx,连续\end{cases}$

方差：反应随机变量的离散程度，$Var(X)=E(X-EX)^2,\sigma(X)=\sqrt{Var(X)}$为标准差

$Var(X+Y)=Var(X)+Var(Y)+2Cov(X,Y)$

随机变量标准化: $Y=\frac{X-EX}{\sqrt{Var(X)}}, EY=0, Var(Y)=1$

Chebyshev ineq. X的方差存在，则对$\forall\varepsilon>0$,

$$P(|X-EX|\geq\varepsilon)\leq\frac{Var(X)}{\varepsilon^2}, P(|X-EX|<\varepsilon)\geq 1-\frac{Var(X)}{\varepsilon^2}$$

常用分布的期望和方差在前面已经讨论过。

协方差: $Cov(X,Y)=E[(X-EX)(Y-EY)]=EXY-EXEY$

若X与Y独立，则$Cov(X,Y)=0$

相关系数: $\rho_{XY}=\frac{Cov(X,Y)}{\sqrt{Var(X)}\sqrt{Var(Y)}}$为$X$和$Y$的相关系数

$\rho_{XY}\in[-1,1]$,越接近1，X与Y正相关；越接近-1，X与Y负相关

Schwarz ineq. $Cov(X,Y)^2\leq Var(X)Var(Y)$

矩: k阶原点矩：EX^k，k阶中心矩：$E[X-E(X)]^k$

$k+l$阶混合矩：EX^kY^l，$k+l$混合中心矩：$E[(X-EX)^k(Y-EY)^l]$

协方差矩阵: $X=(X_1,\cdots,X_n)$,则X的协方差矩阵$Cov(X)$为$\begin{cases}a_{ii}=Var(X_i)\\a_{ij}=Cov(X_i,X_j)\end{cases}$

相关矩阵: R：$r_{ij}=\rho_{ij}$

习题4、习题5

大数定律与中心极限定理

大数定律: 一般形式：若$r.v.$序列$\{X_n\}$满足：$\lim_{n\to\infty}P|\frac{1}{n}\sum_{i=1}^n X_i-\frac{1}{n}\sum_{i=1}^n E(X_i)|<\varepsilon$

则称$\{X_n\}$服从大数定律。

Chebyshev ver. $\{X_n\}$两两不相关，且方差都存在，并且有共同的上界，则服从大数定律。

可用Chebyshev ineq.证明

依概率收敛: 对$\forall\varepsilon>0, \lim_{n\to\infty}P\{|Y_n-Y|<\varepsilon\}=1$,则称$\{Y_n\}$依概率收敛于$Y$.

Bernoulli ver. μ_n为n重Bernoulli试验种事件A出现次数，每次试验中$P(A)=p$,

则对$\forall\varepsilon>0$,有$\lim_{n\to\infty}P\{|\frac{\mu_n}{n}-p<\varepsilon\}=1$

Markov ver. $\{X_n\}$满足$\frac{1}{n}Var(\sum_{i=1}^n X_i)\to 0$,则$\{X_n\}$服从大数定律。

Khinchin ver. $\{X_n\}$独立同分布，且X_n数学期望存在，则$\{X_n\}$服从大数定律

注意：Bernoulli⊂Chebyshev⊂Markov，Bernoulli⊂Khinchin

C.L.T: 独立随机变量和：$Y_n=\sum_{i=1}^n X_i$,中心极限定理即该极限分布均为正态分布

定理：$\{X_n\}i.i.d\ with\ EX=\mu, Var(X)=\sigma^2>0$，$as\ n\to\infty$

$$\lim_{n\to\infty}P\{\frac{Y_n-n\mu}{\sigma\sqrt{n}}\leq x\}=\Phi(x)$$

应用：1）$\frac{Y_n-n\mu}{\sigma\sqrt{n}}\sim N(0,1)$ 2) $\sum_{i=1}^n X_i\sim N(n\mu,n\sigma^2)$ 3) $\bar{X}\sim N(\mu,\frac{\sigma^2}{n})$

注意: 在对二项分布做正态近似时，可有如下修正：

$$P(k_1 \le X \le k_2) = P(k_1 - 0.5 < X < k_2 + 0.5) \approx \Phi(\frac{k_2 + 0.5 - np}{\sqrt{np(1-p)}}) - \Phi(\frac{k_1 - 0.5 - np}{\sqrt{np(1-p)}})$$

应用题中，n, x和P三者可由其二推出剩下一个的值，具体例题见ppt（**习题6**）

二、概率与统计：应用

据往年经验，大概只要简单了解概念就行?

密码学：生日攻击

k个人中存在生日相同的两个人的概率为$1 - \frac{365!}{365^k(365-k)!}$

当人数达到**k=23**时，就有50%以上的概率出现两人生日相同。(往年考过)

应用1：找到冲突的Hash函数值，伪造报文，攻击身份验证算法

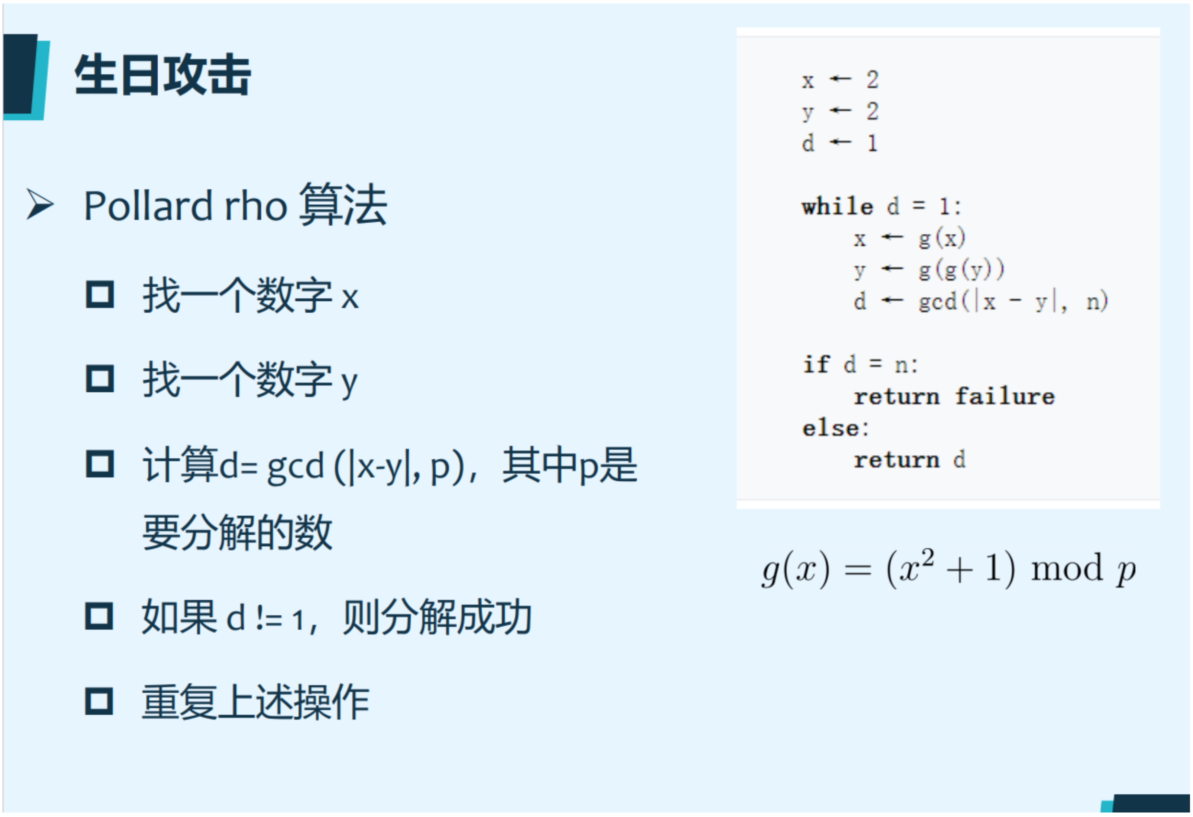
对64位Hash，有$2^{64} \approx 1.8 \times 10^{19}$个输出

仅需5.38×10^9即可生成碰撞，此值称为"**生日界限**"。

防范：设置更长的Hash length

应用2：离散对数：基于同余运算和原根的对数运算

Pollard rho 算法:



防范：找更大的整数，定时更换大整数

三、线性代数与矩阵论

矩阵运算：略

零化度：$Nullity = n - rank(A)$

特征值求法：$det(\lambda I_n - A) = 0$,特征向量求法：$(\lambda I_n - A)x = 0$，x的非零解

正定矩阵：所有特征值大于0

可对角化：若$A=PDP^{-1}$,则P中的列向量是A的特征向量，D中对角元为A的特征值

奇异值分解：$A=U\Sigma V^T$,AA^T，A^TA的特征向量分别构成U,V,特征值开方为Σ中的对角元。

对易式：$[A,B]=AB-BA$,若为零，称为对易的

反对易式：$\{A,B\}=AB+BA$,若为零，称为反对易的

四、线性代数与矩阵论: 应用

量子计算

给出量子计算下的定义：量子比特$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$,要求其模长为1

$$|v\rangle=\begin{pmatrix}v_0\\v_1\\\vdots\\v_{N-1}\end{pmatrix},|w\rangle=\begin{pmatrix}w_0\\w_1\\\vdots\\w_{N-1}\end{pmatrix}$$

$$\langle w|=(w_0^*,w_1^*,\cdots,w_{N-1}^*)$$

则量子意义下的内积

$$\langle w|v\rangle=\langle v|w\rangle^*=\sum_{i=0}^{N-1}w_i^*v_i$$

显然有$\langle v|v\rangle=\sum_{i=0}^{N-1}v_i^*v_i=\sum_{i=0}^{N-1}|v_i|^2=1$

则量子版的柯西-施瓦兹不等式为

$$|\langle\alpha|\beta\rangle|^2\leq\langle\alpha|\alpha\rangle\langle\beta|\beta\rangle$$

将量子版的定义换回正常的定义，就和普通版的证明没什么区别

谱分解：$A=\sum_{j=0}^{N-1}\lambda_j|\mu_j\rangle\langle\mu_j|$,其中$|\mu_j\rangle$为矩阵的第$j$个本征矢，$\lambda_i$为对应本征值

常用泡利阵：

泡利阵记号	别名	矩阵表示	谱分解	作用
I,σ_0		$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\|0\rangle\langle0\|+\|1\rangle\langle1\|$	恒等变换
X,σ_x,σ_1	非门	$\begin{pmatrix}0&1\\1&0\end{pmatrix}$	$\|+\rangle\langle+\|-\|-\rangle\langle-\|$	$\|0\rangle\to\|1\rangle$， $\|1\rangle\to\|0\rangle$
Y,σ_y,σ_2		$\begin{pmatrix}0&-i\\i&0\end{pmatrix}$	$\|p\rangle\langle p\|-\|q\rangle\langle q\|$，其中 $\|p\rangle=\frac{\|0\rangle+i\|1\rangle}{\sqrt{2}}=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}$， $\|q\rangle=\frac{\|0\rangle-i\|1\rangle}{\sqrt{2}}=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}$。	$i\sigma_y$的作用*： $\|0\rangle\to-\|1\rangle$， $\|1\rangle\to\|0\rangle$
Z,σ_z,σ_3		$\begin{pmatrix}1&0\\0&-1\end{pmatrix}$	$\|0\rangle\langle0\|-\|1\rangle\langle1\|$	$\|0\rangle\to\|0\rangle$， $\|1\rangle\to-\|1\rangle$

最小二乘法

只需记住$W=(X^TX)^{-1}X^Ty$

五、微分和差分

微积分内容略

Recall: 条件极值：求在约束$\phi(x,y)=0$条件下函数$z=f(x,y)$的极值

方法1：能解出显式解$y=\psi(x)$，则$z=f(x,\psi(x))$

方法2：拉格朗日乘数法

$$z=f(x,y)\Rightarrow\frac{dz}{dx}=f_x+f_y\frac{dy}{dx}=0\Rightarrow f_x-f_y\frac{\phi_x}{\phi_y}=0$$

引入辅助函数$F=f(x,y)+\lambda\phi(x,y)$

极值点满足

$$F_x=f_x+\lambda\phi_x=0,F_y=f_y+\lambda\phi_y=0,F_\lambda=\phi=0$$

差分

无限微积分：$Df(x)=\lim_{h\to0}\frac{f(x+h)-f(x)}{h}$，作用于连续函数

有限微积分：$\Delta f(x)=f(x+1)-f(x)$,Δ为差分算子，作用于离散函数

下降阶乘幂：$x^{\underline{m}}=x(x-1)\cdots(x-m+1)$

上升阶乘幂：$x^{\overline{m}}=x(x+1)\cdots(x+m-1)$

则差分算子在下降阶乘幂上的结果为$\Delta(x^{\underline{m}})=mx^{\underline{m-1}}$,这与微分$D(x^m)=mx^{m-1}$形式类似

逆差分算子：求和算子$\Sigma:g(x)=\Delta f(x)\quad iff\quad\sum g(x)\delta x=f(x)+C$

这里$\sum_a^b g(x)\delta x=\sum_{k=a}^{b-1}g(k)$

下降幂的求和: $\sum_{0\le k<n}k^{\underline{m}}=\frac{n^{\underline{m+1}}}{m+1}$,这与定积分的结果也是平行的

下降幂指数的推广：$x^{\underline{-m}}=\frac{1}{(x+1)(x+2)\cdots(x+m)}$

结论：

$$\text{对}m\ne-1,\Delta x^{\underline{m}}=mx^{\underline{m-1}},\sum_a^b x^{\underline{m}}\delta x=\frac{x^{\underline{m+1}}}{m+1}|_a^b$$

$m=-1$时呢？调和数：H_x，对lnx的有限模拟

$$H_x=\frac{1}{1}+\frac{1}{2}+\cdots+\frac{1}{x},\Delta H_x=H_{x+1}-H_x=\frac{1}{x+1}=x^{\underline{-1}}$$

可用下降阶乘幂快速计算求和式。

应用：Logistic回归，傅里叶变换，瞄一眼就行。